Paper Reference 20158K
Pearson BTEC
Level 3 Nationals Diploma,
Extended Diploma,

INFORMATION TECHNOLOGY

UNIT 11: CYBER SECURITY AND INCIDENT MANAGEMENT

(PART B)

Window for supervised period:

Monday 7 January 2019 – Friday 25 January 2019

Supervised hours: 4 hours (plus your additional time allowance)

SET TASK BRIEF

X61675A

Pearson

SET TASK BRIEF

CRITICALLY ENDANGERED

Peter Russof is a computer programmer specialising in developing games for PCs. He has written several stand – alone games and has built up a profitable business as an independent game producer.
Peter lives in Watford and works from home.

He has developed Critically Endangered (CE), a multiplayer online game set in a post – apocalyptic world. In CE a plague has caused man to be critically in danger of extinction. Peter's innovative idea was to use real world data such as maps, weather statistics, ecological and geographical information to create play areas. Players select a location in the real world and Peter's algorithms create a 3D play area of that location after the plague. Each player then creates, customises and controls their own player character, using it to interact with the play area and other players.

continued on the next page . . .

**CE has an enthusiastic following of several thousand players with an active online community.
Several of the players help by running a game forum and acting as guides and troubleshooters within the game environment.**

Peter has gone into partnership with his cousin, Elana, who has run Romwebhost, a Romanian web hosting company, since 1998. Peter develops and supports CE while Elana supplies processing and hosting facilities through Romwebhost.

People who wish to play CE must create a user account and then log in via that account in order to access a play area.

---

continued on the next page . . .

CLIENT BRIEF

YOU ADVISED PETER AND ELANA ON SECURITY MATTERS. NOW, A FEW MONTHS LATER, ELANA HAS CALLED YOU IN TO REVIEW THE INVESTIGATION OF A CYBER SECURITY INCIDENT.

In December 2018 Elana received an email from an irate customer, complaining that his CE account had been hacked. Elana investigated the complaint because the customer had sent the email to her personal mailbox rather than the usual Support@CriticallyEndangered.com

Alex, the Cyber Security Manager at Romwebhost, told Elana that there had been an unusually high number of reports of compromised accounts in November 2018. Staff had dealt with the problem in accordance with the Incident Management Policy and Alex had not thought the incident serious enough to escalate further.

As there was a threat of possible legal action in the email, Elana asked Alex to investigate further. The matter was then discussed at a meeting.

Turn over

EVIDENCE ITEMS FROM THE SECURITY INCIDENT AT ROMWEBHOST

Evidence items include:

1) **Cyber Security Manager's report**
2) **Customer email**
3) **Notes from meeting to discuss the incident**
4) **Account security flowchart**
5) **Cyber security document – Incident Management Policy.**

---

continued on the next page . . .

1. CYBER SECURITY MANAGER'S REPORT

COMPROMISED ACCOUNTS, NOVEMBER 2018

COMPROMISE CATEGORIES

There was a higher than normal number of compromised accounts in November.
These fell into three categories:

(a) Account lockouts due to incorrect password attempts. There were 296 instances logged, which is within normal expectations.

(b) Players reporting account penetration with damage to their player character. There were 105 instances. This figure is about 10 times greater than normal expectations. In every instance the damage followed a similar pattern. The player's character was used to create a message and then the character was put in a situation where it died. The message took several different forms, e.g. marked on a wall, scraped on the ground, but was always the same single word, 'Extinct'.

continued on the next page . . .

(c) Players reporting account penetration with effects other than category (b). There were 9 instances. This is within normal expectations. Reported effects varied but were all minor vandalism such as changing the player's name to something derogatory.

COMPROMISE HANDLING METHODS

Category (a) automatically by password recovery/security question system.
Category (b) manually by Support staff.
Category (c) manually by players, reversing the vandalism, with assistance from Support where needed.

ACTIONS TAKEN FOR CATEGORY (b) COMPROMISES

Most reports came via in – game chat, others were emailed to Support.

- The first – line technician logged the incidents.
- The technician was able to restore player characters by using our back – up system.
- The technician received help from the in – game troubleshooters.

- The troubleshooters went into the affected play area to remove any traces of the attack, e.g. remove ‘Extinct’ and restore any damage caused by writing the word.
- Finally, a password change was enforced for the affected account.

ESCALATION OF THE PROBLEM

The technician dealt with several similar cases and followed procedures by escalating the problem to the Duty Manager. The Duty Manager recognised that this was a potentially serious threat and passed it on to the Cyber Security Team.

ACTIONS TAKEN BY THE CYBER SECURITY TEAM

As the damage was easy to reverse, the Cyber Security Team decided to monitor the situation before taking any drastic action.

After a few more days, the Cyber Security Manager noted that:

- the number of compromises per day was increasing

- no way had been found of predicting which accounts would be compromised
- accounts that had been compromised and had their password changed had not been affected again.

He therefore decided to enforce a password change for all players except those already affected.
The change was explained to players as being a routine security precaution.

No further category (b) compromises were reported and the incident was closed.

---

continued on the next page . . .

2. CUSTOMER EMAIL
(IDENTIFYING INFORMATION REMOVED)

To: Elana@romwebhost.com

From: [redacted]

Subject: Hacked account

Great game, but rubbish security. I've only been on your site for a couple of months and already been hacked and killed off. OK, your techs did a nice job of fixing things, but it should never have happened.

You make a big deal out of being an independent and looking after your players but someone's leaked. After all the publicity about the [redacted] **Games and** [redacted] **Online hacks last year, I'd have thought you would have been a bit more careful.**

Repairing the character damage was fine, but what about my personal info? If someone's had my password out of you, they've obviously got a load of personal info as well. No one's said they'll do anything about that.

[redacted] **Games at least offered identity theft insurance for a year and** [redacted] **Online gave me a free year's subscription. What are you doing?**

You're based in Europe and they've got some tough data protection laws there, so you need to get moving on this before my lawyers get on the case.

Mr [redacted]

---

continued on the next page . . .

3. NOTES FROM THE MEETING TO DISCUSS THE INCIDENT

Those present; Peter, Elana, Alex, Maria (Romwebhost Legal Department)

Elana: Called meeting to order, asked Maria for legal opinion.

Maria: Mr [redacted] lives in New York, we have no physical presence in the USA, so a lawsuit is unlikely. Seems probable he is looking for a small payout in line with [redacted] Games and [redacted] Online.

Data protection penalties only apply if passwords were obtained from us, but an investigation would be expensive.

Legal Department needs to know if:

- **passwords could have been stolen, by staff or external agent**
- **our security methods took into account what happened at [redacted] Games and [redacted] Online.**

Alex: We wanted to get CE off to a good start, so had a separate physical server to the Romwebhost hosting business. We only used a few, experienced staff as technicians for CE. Theft by staff has a low probability. The security measures for player accounts were ported from Peter's previous version of the game.

Peter: I was aware of the [redacted] Games and [redacted] Online hacks, and several previous ones. I designed the system to be secure and not vulnerable to those hacks. (ACCOUNT SECURITY FLOWCHART, EVIDENCE ITEM 4, HANDED OUT.)

In the [redacted] Games hack they stored passwords as plain text and relied on the database being secure. Someone did some database maintenance and left it linked to the internet. The hacker downloaded everything. The data went on sale for anyone to buy. We only store hashes.

continued on the next page . . .

In the [redacted] Online hack I've heard that it was an SQL injection attack, we filter all our inputs so are protected there. [redacted] Online encrypted passwords and stored hashes like us, but only used the MD5 hashing algorithm. I moved the CE system to SHA2 some years ago. A sample of the [redacted] Online hashes was circulated, but then everything went quiet. Rumour says that [redacted] Online paid a ransom.

Alex: We checked the SQL filters and server security after the attack and everything was still in place. For obvious reasons, I don't think it was a brute force attack.

Elana: Summing up, we think we're still secure and are not legally liable. Just to be safe, we should ask someone from outside the company to review the incident.

Others: Agree.

---

continued on the next page . . .

4. ACCOUNT SECURITY FLOWCHART

Look at the diagram for section 4 in the separate Diagram Booklet.
The diagram shows a flowchart for the account security.

Notes.

i. **Username is pre – populated from player's email address. This can be changed but most player's don't do that. Password must be a minimum of 8 characters.**

ii. **SQL uniqueidentifier is a 16 byte string generated by the computer on which the SQL database is running. It is globally unique (cannot be generated as uniqueidentifier by any other computer in the world). Using a salt prevents lookup table attacks.**

iii. **Only the hash, salt and username are stored. The password is discarded.**

---

continued on the next page . . .

5. CYBER SECURITY DOCUMENTATION – INCIDENT MANAGEMENT POLICY

INCIDENT MANAGEMENT TEAM

The Computer Security Incident Response Team (CSIRT) will be formed from the Cyber Security Team at Romwebhost.

The CSIRT will include:

- **the first – line technician on duty at the time of the incident**
- **the Cyber Security Manager**
- **members of the Cyber Security Team nominated by the Cyber Security Manager.**

INCIDENT REPORTING

Any member of staff who considers that an IT – related security incident has occurred must report it as soon as possible to their line manager.
The manager will assess the threat and escalate it to the CSIRT leader if they consider it to be serious. Initially it may be reported verbally but this must be followed up by an email. It is the responsibility of the

CSIRT to maintain detailed documentation on the incident from first report to final resolution.

Security incidents may include:

- **theft of IT equipment**
- **theft of company data**
- **unauthorised access to company IT systems**
- **infection of company IT systems with malware.**

INCIDENT RESPONSE PROCEDURES

(a) THEFT OF IT EQUIPMENT

- **Theft of IT equipment is a very serious issue. Any thefts must be reported at once to the CSIRT leader, initially a verbal report must be made followed up by email, providing as much information as possible (location and type of equipment, when it was last seen, etc.).**
- **The CSIRT team leader must ascertain if the item has actually been stolen (or if it is just missing).**
- **If the item is confirmed as stolen, CSIRT team leader must inform the police and contact the finance department so they can inform insurers.**

- **The CSIRT must prepare a report on the theft to Romwebhost senior management and if needed justify the finances required to replace the stolen item.**

(b) THEFT OF COMPANY DATA

- **Theft or loss of company data equipment may occur in a number of different ways.**
- **Any loss of company data must be reported at once to CSIRT team leader, initially a verbal report must be made followed up by email.**
- **The CSIRT must investigate the loss and identify exactly what data has been lost or stolen and when the incident occurred.**
- **Having identified what has been lost or stolen and when, the CSIRT must retrieve backups and restore the data as soon as possible.**
- **The CSIRT should review the incident and implement procedures to prevent future losses.**

continued on the next page . . .

(c) INFECTION OF COMPANY IT SYSTEMS WITH MALWARE

Any member of staff who suspects that any IT system has been infected with malware must:

- **Report at once to the CSIRT team leader, initially a verbal report must be made followed up by email.**
- **The infected system should be shut down as soon as possible.**
- **The CSIRT will investigate the infection and take appropriate measures to resolve the infection and restore the system.**

(d) UNAUTHORISED ACCESS TO COMPANY SYSTEMS

- **Any member of staff who suspects that there has been unauthorised access to any Romwebhost IT system must report it at once to their line manager.**
- **The manager will assess the situation and, if unauthorised access is confirmed, escalate the report to the CSIRT team leader, providing as much detail as possible (which system, how access was obtained). Initially a verbal report must be made, followed up by email.**

- **The CSIRT will thoroughly investigate the incident and identify how the unauthorised access was obtained.**
- **The CSIRT will take whatever action is required to prevent future occurrences.**

  A report must be sent to Romwebhost senior management.